VPN 원격 사무실/스포크의 ZTD(Zero Touch Deployment) 구성

목차

소개

이 문서에서는 ZTD(Zero Touch Deployment) 옵션이 구축을 위한 비용 효율적이고 확장 가능한 솔루션인 방법에 대해 설명합니다.

안전하고 효율적인 배포와 Remote Office 라우터(Spoke라고도 함)의 프로비저닝은 어려운 작업입니다.원격 사무소는 현장 엔지니어가 라우터를 현장 구성하도록 하는 것이 어려운 위치에 있을 수 있으며, 대부분의 엔지니어는 비용 및 잠재적 보안 위험 때문에 사전 구성된 스포크 라우터를 전송하지 않도록 선택할 수 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- USB 플래시 드라이브를 지원하는 USB 포트가 있는 모든 Cisco IOS® 라우터자세한 내용은 USB eToken 및 USB Flash 기능 지원을 참조하십시오.
- 이 기능은 거의 모든 Cisco 8xx 플랫폼에서 작동하는 것으로 확인되었습니다.자세한 내용은 기

본 구성 파일 백서(Cisco 800 Series ISR의 기능 지원)를 참조하십시오.

- ISR(Integrated Service Router) 시리즈 G2 및 43xx/44xx와 같은 USB 포트가 있는 기타 플랫폼.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

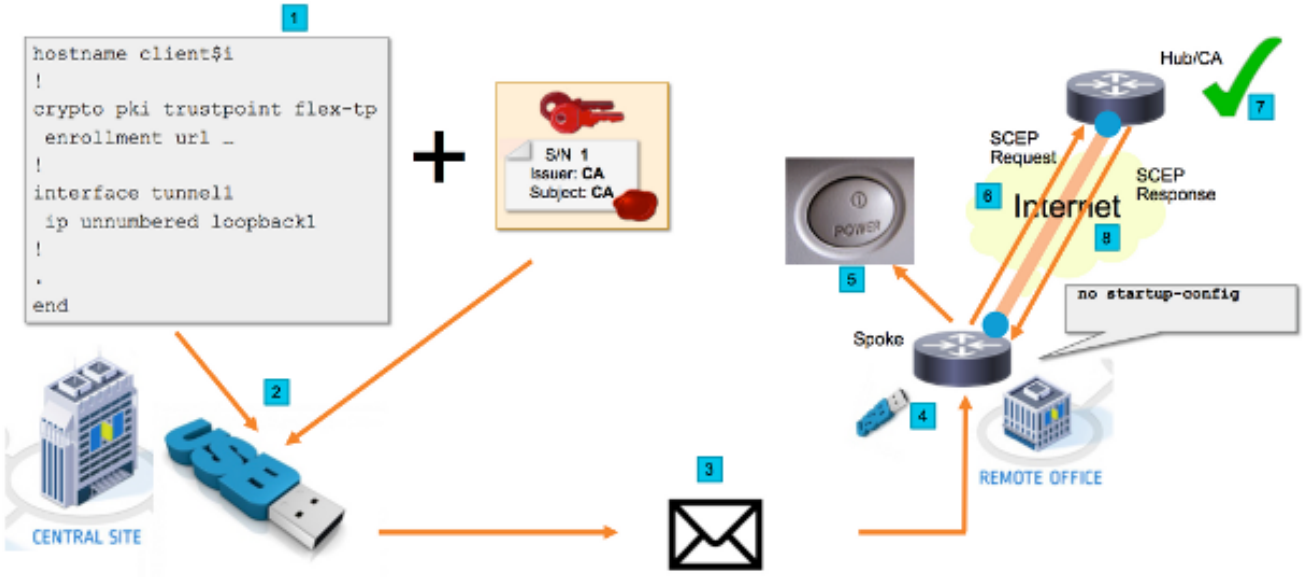
- SCEP(Simple Certificate Enrollment Protocol)
- USB를 통한 제로 터치 구축
- DMVPN/FlexVPN/사이트 간 VPN

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

참고:이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램



네트워크 흐름

1. 중앙 사이트(회사의 본사)에서 스포크 컨피그레이션의 템플릿이 생성됩니다.템플릿에는 VPN 허브 라우터의 인증서를 서명한 CA(Certificate Authority) 인증서가 포함되어 있습니다.
2. 구성 템플릿은 ciscortr.cfg라는 파일의 USB 키**에서 인스턴스화됩니다**.이 구성 파일에는 구축할 라우터에 대한 스포크 특정 컨피그레이션이 포함되어 있습니다. **참고:**USB의 컨피그레이션에는 IP 주소 및 CA 인증서 이외의 중요한 정보가 포함되지 않습니다.Spoke 또는 CA 서버의 개인 키가 없습니다.

3. USB 플래시 드라이브는 우편 또는 패키지 배달 회사를 통해 원격 사무실로 전송됩니다.
4. Spoke 라우터는 Cisco Manufacturing에서 직접 원격 사무실로 전송됩니다.
5. 원격 사무실의 라우터는 USB 플래시 드라이브에 포함된 지침에 설명된 대로 전원이 연결되고 네트워크에 연결되어 있습니다.다음으로 USB 플래시 드라이브가 라우터에 삽입됩니다. **참고:**이 단계에는 기술 기술이 거의 없거나 전혀 없기 때문에 모든 사무실 직원이 쉽게 수행할 수 있습니다.
6. 라우터가 부팅되면 usbflash0:/ciscortr.cfg에서 컨피그레이션**을 읽습니다**.라우터의 전원이 켜지면 SCEP(Simple Certificate Enrollment Protocol) 요청이 CA 서버로 전송됩니다.
7. CA 서버에서 Manual(수동) 또는 Automatic Granting(자동 부여)은 회사 보안 정책에 따라 구성할 수 있습니다.수동 인증서 부여를 위해 구성된 경우 SCEP 요청의 대역 외 확인을 수행해야 합니다(IP 주소 검증 확인, 구축을 수행하는 직원에 대한 자격 증명 검증 등). 이 단계는 사용되는 CA 서버에 따라 다를 수 있습니다.
8. 이제 유효한 인증서가 있는 스포크 라우터에서 SCEP 응답을 수신하면 IKE(Internet Key Exchange) 세션이 VPN 허브로 인증되고 터널이 성공적으로 설정됩니다.

SUDI 기반 권한 부여

7단계에는 SCEP 프로토콜을 통해 전송된 인증서 서명 요청을 수동으로 확인하는 과정이 포함되며 , 기술 외적인 인력에게 수행하기가 번거롭고 어려울 수 있습니다.보안을 강화하고 프로세스를 자동화하려면 SUDI(Secure Unique Device Identification) 디바이스 인증서를 사용할 수 있습니다 .SUDI 인증서는 ISR 4K 디바이스에 내장된 인증서입니다.이러한 인증서는 Cisco CA에서 서명합니다.제조된 각 장치는 서로 다른 인증서로 발급되었으며 디바이스의 일련 번호는 인증서의 일반 이름 내에 포함됩니다.SUDI 인증서, 관련 키 쌍 및 전체 인증서 체인은 변조 방지 Trust Anchor 칩에 저장됩니다.또한 키 쌍은 특정 Trust Anchor 칩에 암호로 바인딩되며 개인 키는 내보내지 않습니다 .이 기능을 사용하면 ID 정보를 복제하거나 스푸핑할 수 없습니다.

SUDI 개인 키를 사용하여 라우터에서 생성한 SCEP 요청에 서명할 수 있습니다.CA 서버는 서명을 확인하고 디바이스의 SUDI 인증서의 내용을 읽을 수 있습니다.CA 서버는 SUDI 인증서(예: 일련 번호)에서 정보를 추출하고 해당 정보를 기반으로 권한 부여를 수행할 수 있습니다.RADIUS 서버를 사용하여 이러한 권한 부여 요청에 응답할 수 있습니다.

관리자는 스포크 라우터 및 관련 일련 번호 목록을 생성합니다.일련 번호는 기술 담당자가 아닌 라우터의 케이스에서 읽을 수 있습니다.이러한 일련 번호는 RADIUS 서버 데이터베이스에 저장되며 서버는 해당 정보를 기반으로 SCEP 요청을 승인하며, 이 정보를 통해 인증서를 자동으로 부여할 수 있습니다.일련 번호는 Cisco 서명 SUDI 인증서를 통해 특정 장치에 암호로 연결되어 있으므로 위조할 수 없습니다.

요약하면, CA 서버는 다음 조건을 모두 충족하는 요청을 자동으로 부여하도록 구성됩니다.

- Cisco SUDI CA에서 서명한 인증서와 연결된 개인 키로 서명됨
- SUDI 인증서에서 가져온 일련 번호 정보를 기반으로 RADIUS 서버에서 권한을 부여

구축 시나리오

CA 서버가 인터넷에 직접 노출될 수 있으므로 터널을 구축하기 전에 클라이언트가 등록을 수행할 수 있습니다.CA 서버는 VPN 허브와 동일한 라우터에 구성할 수도 있습니다.이 토폴로지의 장점은 단순성입니다.CA 서버가 인터넷을 통해 다양한 형태의 공격에 직접 노출되므로 보안의 단점은 줄어듭니다.

또는 Registration Authority 서버를 구성하여 토폴로지를 확장할 수 있습니다.등록 기관 서버 역할은 유효한 인증서 서명 요청을 평가하고 CA 서버에 전달하는 것입니다.RA 서버 자체는 CA의 개인 키를 포함하지 않으며 자체적으로 인증서를 생성할 수 없습니다.이러한 구축에서 CA 서버를 인터

넷에 노출하지 않아도 되므로 전반적인 보안이 향상됩니다.'

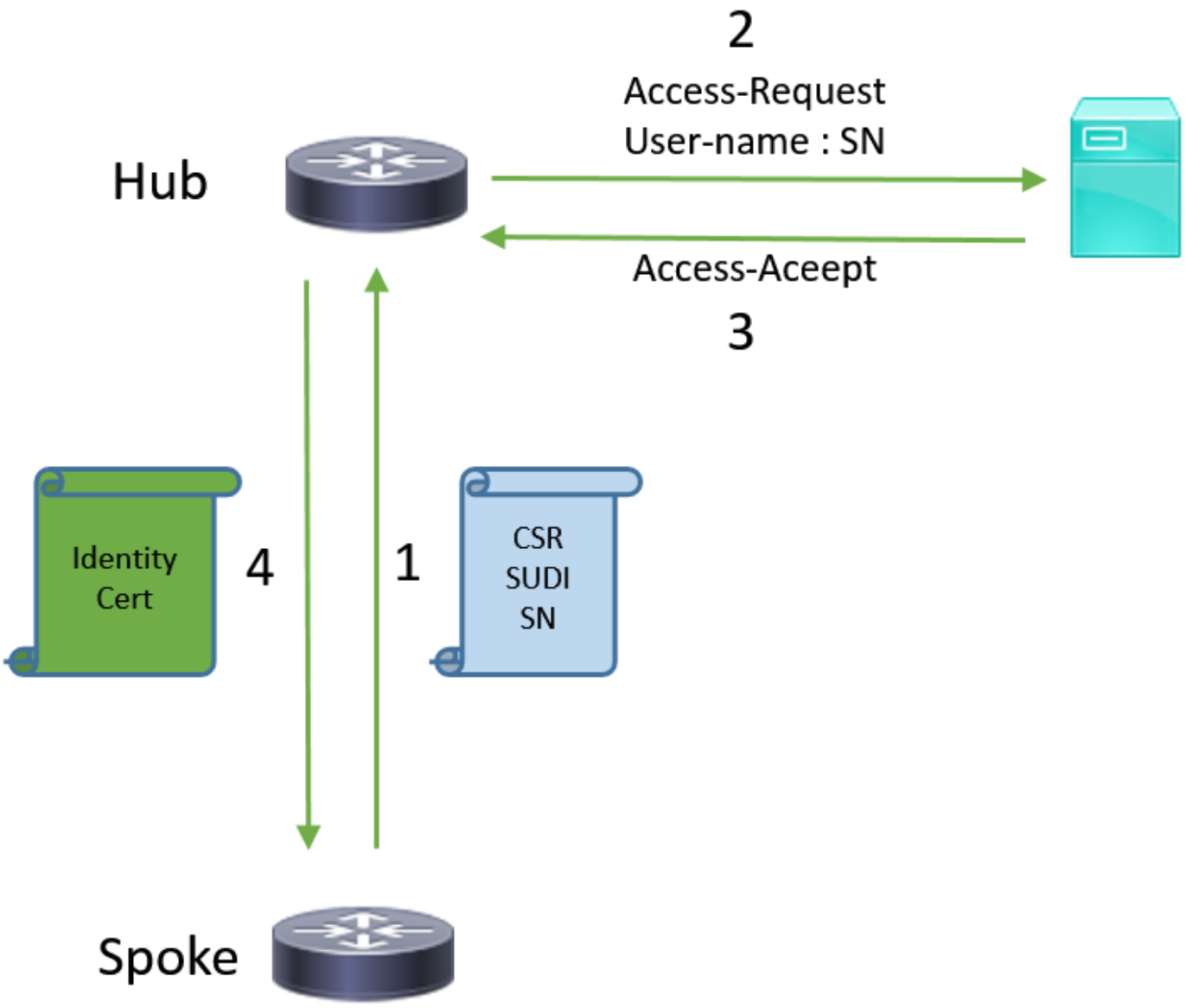
네트워크 흐름

1. 스포크 라우터가 SCEP 요청을 생성하고 SUDI 인증서의 개인 키로 서명하여 CA 서버로 전송합니다.

2. 요청이 올바르게 서명된 경우 RADIUS 요청이 생성됩니다.일련 번호는 사용자 이름 매개 변수로 사용됩니다.

3. RADIUS 서버가 요청을 수락하거나 거부합니다.

4. 요청이 수락되면 CA 서버가 요청을 부여합니다.거부된 경우 CA 서버는 "Pending(보류 중)" 상태로 응답하고, 클라이언트는 대체 타이머가 만료된 후 요청을 재시도합니다.



CA 전용 구성

```
!CA server
```

```
radius server RADSRV
address ipv4 10.10.20.30 auth-port 1812 acct-port 1813
key cisco123

aaa group server radius RADSRV
server name RADSRV

aaa authorization network SUDI group RADSRV

crypto pki server CA
! will grant certificate for requests signed by SUDI certificate automatically
grant auto trustpoint SUDI
issuer-name CN=ca.example.com
hash sha256
lifetime ca-certificate 7200
lifetime certificate 3600

crypto pki trustpoint CA
rsakeypair CA 2048

crypto pki trustpoint SUDI
! Need to import the SUDI CA certificate manually, for example with "crypto pki import" command
enrollment terminal
revocation-check none
! Authorize with Radius server
authorization list SUDI
! SN extracted from cert will be used as username in access-request
authorization username subjectname serialnumber
```

!CLIENT

```
crypto pki trustpoint FLEX
enrollment profile PROF
! Serial-number, fqdn and ip-address fields need to be defined, otherwise the interactive prompt
will prevent the process from starting automatically
serial-number none
fqdn none
ip-address none
! Password needs to be specified to automate the process. However, it will not be used by CA
server
password 7 110A1016141D5A5E57
subject-name CN=spoke.example.com
revocation-check none
rsakeypair FLEX 2048
auto-enroll 85 crypto pki profile enrollment PROF ! CA server address enrollment url
http://192.0.2.1 enrollment credential CISCO_IDEVID_SUDI ! By pre-importing CA cert you will
avoid “crypto pki authenticate” step. If auto-enroll is configured, enrollment will also start
automatically crypto pki certificate chain FLEX certificate ca 01 30820354 3082023C A0030201
02020101 300D0609 2A864886 F70D0101 04050030 3B310E30 0C060355 040A1305 43697363 6F310C30
0A060355 040B1303 54414331 ----- output truncated ---- quit
```

RADIUS server:

The Radius needs to return Access-Accept with the following Cisco AV Pair to enable certificate enrollment:

```
pki:cert-application=all
```

CA 및 RA를 통한 구성

!CA server

```
crypto pki server CATEST
   issuer-name CN=CATEST.example.com,OU=TAC,O=Cisco
   ! will grant the requests coming from RA automatically
   grant ra-auto
crypto pki trustpoint CATEST
   revocation-check crl
   rsakeypair CATEST 2048
```

!RA server

```
radius server RADSRV
   address ipv4 10.10.20.30 auth-port 1812 acct-port 1813
   key cisco123

aaa group server radius RADSRV
   server name RADSRV

aaa authorization network SUDI group RADSRV

crypto pki server RA
   no database archive
   ! will forward certificate requests signed by SUDI certificate automatically
   grant auto trustpoint SUDI
   mode ra

crypto pki trustpoint RA
   ! CA server address
   enrollment url http://10.10.10.10
   serial-number none
   ip-address none
   subject-name CN=ra1.example.com, OU=ioscs RA, OU=TAC, O=Cisco
   revocation-check crl
   rsakeypair RA 2048

crypto pki trustpoint SUDI
   ! Need to import the SUDI CA certificate manually, for example with "crypto pki import"
command
   enrollment terminal
   revocation-check none
   ! Authorize with Radius server
   authorization list SUDI
   ! SN extracted from cert will be used as username in access-request
   authorization username subjectname serialnumber
```

!CLIENT

```
crypto pki trustpoint FLEX
   enrollment profile PROF
   ! Serial-number, fqdn and ip-address fields need to be defined, otherwise the interactive
prompt will prevent the process from starting automatically
   serial-number none
   fqdn none
   ip-address none
   ! Password needs to be specified to automate the process. However, it will not be used by CA
server
   password 7 110A1016141D5A5E57
   subject-name CN=spoke.example.com
   revocation-check none
```

```
   rsakeypair FLEX 2048
   auto-enroll 85

crypto pki profile enrollment PROF
   ! RA server address
   enrollment url  http://192.0.2.1
   enrollment credential CISCO_IDEVID_SUDI


! By pre-importing CA cert you will avoid “crypto pki authenticate” step. If auto-enroll is
configured, enrollment will also start automatically
crypto pki certificate chain FLEX
   certificate ca 01
  30820354 3082023C A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  3B310E30 0C060355 040A1305 43697363 6F310C30 0A060355 040B1303 54414331
 ----- output truncated ----
  quit
```

```
RADIUS server:

The Radius needs to return Access-Accept with the following Cisco AV Pair to enable certificate
enrollment:

pki:cert-application=all
```

구성/템플릿

이 샘플 출력은 usbflash **0:/ciscortr.cfg** 파일의 플래시 드라이브에 있는 모범 FlexVPN Remote Office 컨피그레이션을 보여줍니다.

```
hostname client1
!
interface GigabitEthernet0
 ip address dhcp
!
crypto pki trustpoint client1
! CA Server's URL
 enrollment url http://10.122.162.242:80
! These fields needs to be filled, to avoid prompt while doing enroll
! This will differ if you use SUDI, please see above
serial-number none
 ip-address none
 password
 subject-name cn=client1.cisco.com ou=cisco ou
!
crypto pki certificate chain client1
 certificate ca 01
 ! CA Certificate here
       quit
!
crypto ikev2 profile default
 match identity remote any
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint client1
 aaa authorization group cert list default default
!
```

```
interface Tunnel1
 ip unnumbered GigabitEthernet0
 tunnel source GigabitEthernet0
 tunnel mode ipsec ipv4
! Destination is Internet IP Address of VPN Hub
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default
!
event manager applet import-cert
! Start importing certificates only after 60s after bootup
! Just to give DHCP time to boot up
 event timer watchdog time 60
 action 1.0 cli command "enable"
 action 2.0 cli command "config terminal"
! Enroll spoke's certificate
 action 3.0 cli command "crypto pki enroll client1"
! After enrollement request is sent, remove that EEM script
 action 4.0 cli command "no event manager applet import-cert"
 action 5.0 cli command "exit"
event manager applet write-mem
 event syslog pattern "PKI-6-CERTRET"
 action 1.0 cli command "enable"
 action 2.0 cli command "write memory"
 action 3.0 syslog msg "Automatically saved configuration"
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

Spoke(스포크)에서 터널이 작동되었는지 확인할 수 있습니다.

```
client1#show crypto session
Crypto session current status

Interface: Tunnel1
Profile: default
Session status: UP-ACTIVE
Peer: 172.16.0.2 port 500
 Session ID: 1
 IKEv2 SA: local 172.16.0.1/500 remote 172.16.0.2/500 Active
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
       Active SAs: 2, origin: crypto map
```

인증서가 올바르게 등록되었는지 Spoke에서 확인할 수도 있습니다.

```
client1#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=CA
  Subject:
    Name: client1
    hostname=client1
    cn=client1.cisco.com ou=cisco ou
  Validity Date:
```

```
    start date: 01:34:34 PST Apr 26 2015
    end   date: 01:34:34 PST Apr 25 2016
  Associated Trustpoints: client1
  Storage: nvram:CA#6.cer

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=CA
 Subject:
   cn=CA
 Validity Date:
   start date: 01:04:46 PST Apr 26 2015
   end   date: 01:04:46 PST Apr 25 2018
 Associated Trustpoints: client1
 Storage: nvram:CA#1CA.cer
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

알려진 주의 사항 및 문제

Cisco 버그 ID CSCuu93989 - 컨피그레이션 마법사가 G2 플랫폼에서 PnP 플로우를 중지하면 시스템이 usbflash:/ciscortr.cfg에서 컨피그레이션을 로드하지 않을 수 있습니다.대신 컨피그레이션 마법사 기능에서 시스템이 중지될 수 있습니다.

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:
```

참고:이 결함에 대한 수정이 포함된 버전을 사용해야 합니다.

USB를 통한 ZTD와 기본 구성 파일 비교

이 문서에서 사용하는 **기본 구성 파일** 기능은 Cisco 800 Series ISR 구축 개요에 설명된 **USB를 통한 제로 터치 배포와** 다른 기능입니다.

-	**USB를 통한 제로 터치 구축**	**기본 구성 파일**
지원되는 플랫폼	8xx 라우터가 거의 없습니다. 자세한 내용은 Cisco 800 Series ISR 구축 개요를 참조하십시오.	모든 ISR G2, 43xx 및 44xx.
파일 이름	*.cfg	ciscortr.cfg
로컬 플래시에 컨피그레이션을 저장합니다.	예, 자동으로	아니요, EEM(Embedded Ev Manager) 필요

기본 구성 **파일** 기능에서 지원되는 플랫폼이 **더** 많으므로 이 기술은 이 문서에 제시된 솔루션에 대해 선택되었습니다.

요약

USB 기본 구성(USB 플래시 드라이브에서 ciscortr.**cfg** 파일 이름)은 네트워크 관리자가 원격 위치의 장치에 로그인하지 않고도 Remote Office Spoke 라우터 VPN을 구축할 수 있는 기능을 제공합니다(VPN에만 국한되지 않음).

관련 정보

- SCEP(Simple Certificate Enrollment Protocol)
- USB를 통한 제로 터치 구축
- DMVPN/FlexVPN/사이트 간 VPN
- 기술 지원 및 문서 – Cisco Systems
- Cisco 앵커 기술